Services van Windows XP

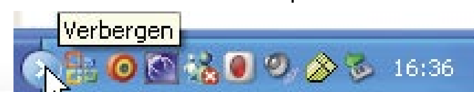
Tot uw dienst!

Naast je eigen toepassingen draait op je systeem ongemerkt ook heel wat Windows-eigen software! Een belangrijk deel hiervan zijn de zogenoemde 'services'. Wat zijn dat, waar vind je ze, wat doen ze, en vooral: wat doe jíj ermee? TOON VAN DAELE

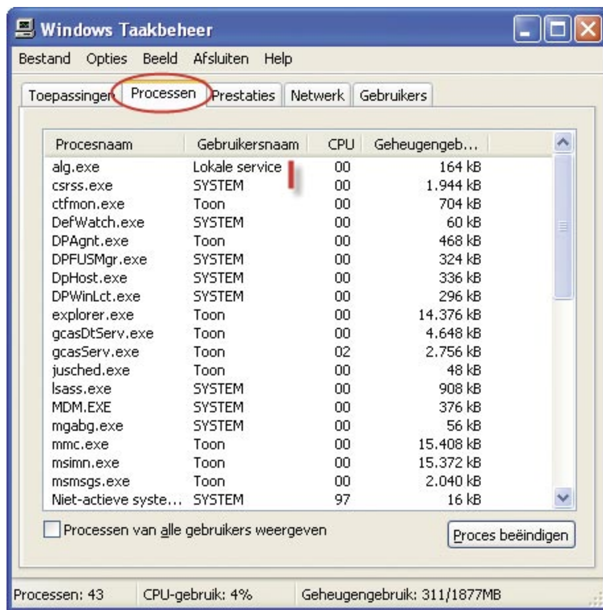
Wie wil uitvissen wat er zoal 'op de achtergrond' actief is tijdens een Windows-sessie, is snel geneigd de taakbalk op het bureaublad te raadplegen. Helemaal rechts tref je namelijk het systeemgebied aan, en daar prijken de icoontjes van allerlei toepassingen die in het geheugen geladen zijn. Nog meer exemplaren duiken op als je het pijlknopje **Verborgen pictogrammen weergeven** indrukt. Dat zijn de icoontjes van toepassingen die wel geladen zijn, maar de gebruiker op dat moment niks speciaals te vertellen hebben. Als je nu dacht dat je hiermee een overzicht van alle actieve software in handen hebt, zit je er dik naast! Deze programmaatjes zijn slechts het topje van de ijsberg: op de achtergrond draaien naast enkele kernbestanden van Windows namelijk nog een reeks stuurprogramma's én flink wat services. Die eerste categorie is je ongetwijfeld wel bekend: bij het installeren van een nieuw brokje hardware moet je namelijk heel vaak zo'n programmaatje (driver) mee installeren. Dat is nodig om Windows veilig met die hardware te laten communiceren in een omgeving waar soms verschillende toepassingen tegelijk eenzelfde apparaat willen aanspreken. Toegang tot dit apparaatbeheer en de bijhorende stuurprogramma's krijg je (onder meer) door de opdracht 'devmgmgt.msc' in te tikken bij **Start, Uitvoeren.**

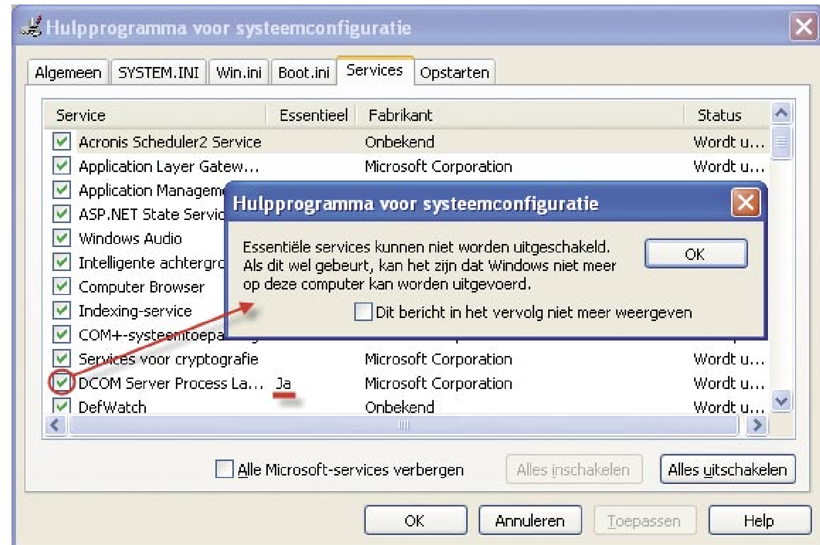
Minder bekend – want meestal goed verborgen – is de tweede categorie: de services.

Dat zijn toepassingen die op een of andere manier de functionaliteit van Windows en andere programma's uitbreiden. Deze services draaien echter op de achtergrond, en zijn dus in principe onzichtbaar voor de gewone gebruiker. Jammer eigenlijk, want het loont de moeite meer zicht én greep te hebben op deze geheimzinnige processen – al was het maar om problematische ser-



(Verborgen) pictogrammen: het topje van de ijsberg.





Weinig nieuws op het servicefront.

De mee-eters van Windows.

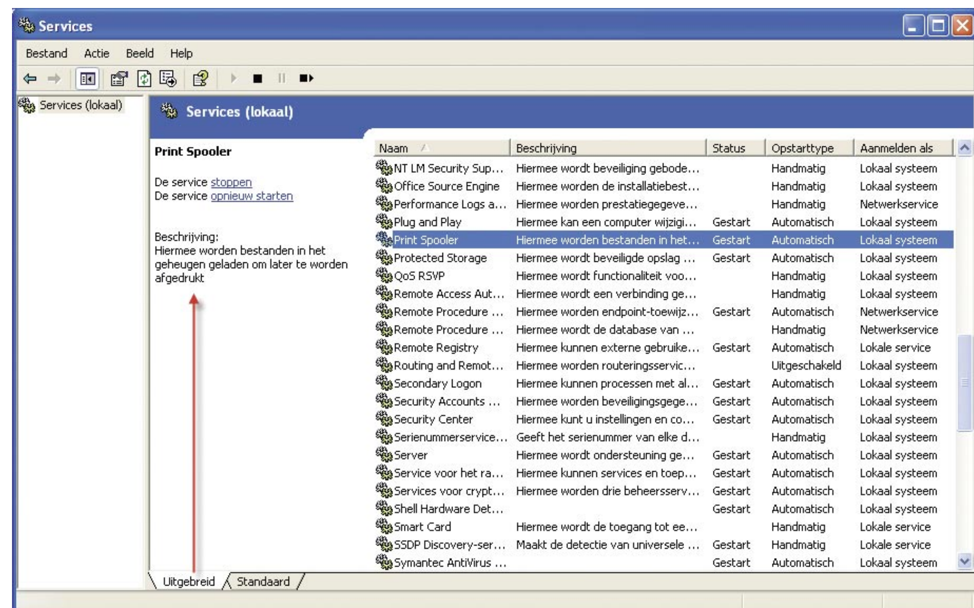
vices weer aan te zwengelen of om overbodige (en niet altijd even veilige!) services tijdelijk op non-actief te zetten... Voor we aan de slag gaan, toch nog even dit: het kunst- en vliegwerk waar we ons in dit dossier aan begeven, is alleen maar mogelijk als je je bij Windows aanmeldt met beheerderrechten.

Boven water

Gelukkig heeft Windows zelf een paar tools aan boord waarmee je die services boven water kan halen. Beginnen we bij het taakbeheer, dat je activeert met de toetsencombinatie **Ctrl+Alt+Delete**. Op het tabblad **Toepassingen** tref je ongeveer dezelfde items aan als de programmabalkjes die zich op de Windows taakbalk bevinden. Om services op te vissen, moet je echter op het tabblad **Processen** zijn. Het komt er ongeveer op neer dat de meeste items waarbij je in de kolom **Gebruikersnaam** geen bekende accountnaam ziet verschijnen, services zijn. Het taakbeheer is echter bijzonder karig met informatie: veel meer dan een cryptische procesnaam en het processor- en geheugengebruik moet je hier niet verwachten. Over dan maar naar een iets loslippiger tool: Msconfig. Die start je op door de gelijknamige opdracht in te tikken bij **Start, Uitvoeren**. Op het tabblad **Opstarten** krijg je dan een keurig overzicht van zowat alle mee-eters: programmaatjes dus die – vaak ongemerkt – samen met Windows opstarten. Services tref je hier echter niet aan; daarvoor moet je op het gelijknamige tabblad zijn. Microsoft is hier gelukkig al iets kwistiger met informatie. De namen van de services zijn minder cryptisch en je verneemt alvast ook wie de fabrikant is. Overigens kan je alle Microsoft-services in één klap onzichtbaar maken door een vinkje te plaatsen naast **Alle Microsoft-services verbergen**: best wel nuttig, want zo krijg je de facto een overzicht van achteraf bijgekomen exemplaren. Verder lees je ook af of de service werkelijk actief is dan wel (tijdelijk) gestopt. Handig is ook dat je van hieruit services kan uitschakelen, zodat ze ook niet langer mee opstarten met Windows. Het volstaat daarvoor het vinkje naast zo'n service te verwijderen. Windows voorkomt echter al te zware blunders door je niet toe te laten essentiële services op deze manier uit te schakelen. Het is trouwens überhaupt geen goed idee om via Msconfig met services te jongleren: deze tool geeft je immers geen erg gedetailleerde informatie, en bovendien zijn er elegantere en veiligere alternatieven om een service op non-actief te zetten...

Beheermodule

Wil je écht met services aan de slag, dan moet je zwaarder geschut bovenhalen. Dat vind je in de vorm van een typische beheermodule van Windows. Die krijg je aan de praat via het **Configuratiescherm** (waar je achtereenvolgens **Prestaties en onderhoud**, **Systeembeheer** en **Services** aanklikt), maar het gaat iets sneller als je bij **Uitvoeren** de opdracht 'services.msc' intikt. In een venster krijg je dan alle geïnstalleerde services opgesomd, en in eerste instantie lijkt de informatie een combinatie te zijn van wat het taakbeheer en Msconfig je al konden vertellen. Je mist hier wel de naam van de fabrikant en of het om een noodzakelijke service gaat, maar de uitgebreide beschrijving bij de meeste services maakt



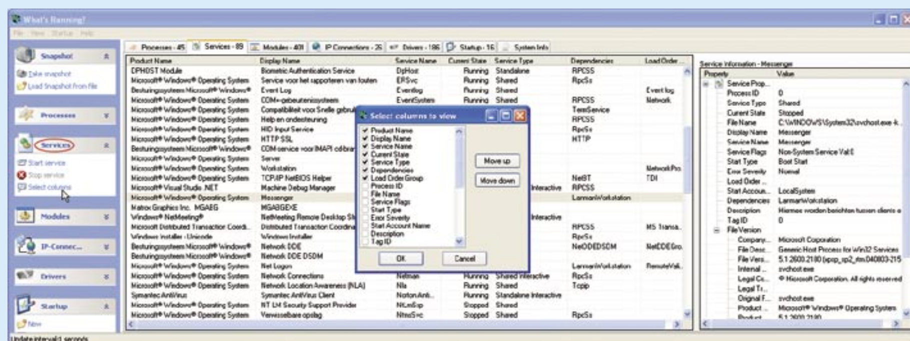
Delicaat werk vraagt aangepast materiaal...



LET OP WELKE SERVICES JE UITSCHAKELT..

DAAR LOOPT WAT!

Wil je het fenomeen services ten gronde onderzoeken, dan kan het gratis tooltje What's Running? www.whatsrunning.net handig van pas komen. Je hoeft hier maar het tabblad **Services** aan te klikken, en je krijgt alle mogelijke informatie over de geïnstalleerde services te zien. Bijkomende gegevens kan je trouwens altijd nog opvragen via de optie **Select columns**. Selecteer je een service, dan verschijnt uiterst rechts nog meer gedetailleerde informatie – vergeet hier niet de plusjes aan te klikken naast **Service Properties** en **File Version**. Overigens kan je vanuit deze tool ingeschakelde services ook stopzetten en (weer) opstarten. Handig is de mogelijkheid om via **Take snapshot** een momentopname van al deze informatie te bewaren. Via de optie **Load Snapshot from file** kan je die dan achteraf vergelijken met de actuele toestand. Oh ja, de tool toont lang niet alleen de services: er zijn ook tabbladen voor **Processes**, **Modules** (dll-bestanden), **IP Connections**, **Drivers**, **Startup** en **System Info**! Een weelde aan interessante gegevens dus – tenminste voor wie weet wat ermee te doen.



heel wat goed. Deze uitleg krijg je trouwens leesbaarder gepresenteerd als je onderaan het tabblad **Uitgebreid** opent. Nieuw is ook de kolom **Opstarttype**. Daaruit leid je al meteen af of een service uitgeschakeld – deze exemplaren kreeg je trouwens niet te zien bij de andere tools – of operationeel is. Hierbij maak je dan nog het onderscheid tussen services die automatisch actief geworden zijn bij het opstarten van Windows en services die klaarstaan in de coulissen om 'handmatig' opgestart te worden. Dat betekent dat die door een gebruiker, door een programma of door een andere service opgestart kunnen worden als dat nodig blijkt. De informatie uit deze beheermodule kan je via het knopje **Lijst exporteren** eventueel ook in een afdrukbaar tekstbestand gieten.

In soorten

Voor we je echter vertellen hoe je services kan manipuleren, bekijken we eerst even welke services er zoal zijn en wat ze op je systeem uitspoken. Dat het er véél zijn, heb je alvast gemerkt: een verse installatie van Windows XP Service Pack 2 levert bijvoorbeeld al zo'n 80 services op, waarvan bijna de helft automatisch wordt opgestart!

Met wat goede wil kan je deze services in een handvol categorieën opsplitsen. Een aantal services neemt de beveiliging van je systeem ter harte. Typische voorbeelden zijn **Automatische updates** (die op gezette tijden *patches* van Microsoft kan binnenhalen) en het **Security Center** (dat updates, antivirusinformatie en firewall centraliseert). Andere services trachten vooral het netwerkverkeer te stroomlijnen en zullen dus vooral hun nut bewijzen als je pc zich in een thuisnetwerkje bevindt. We noemen hier exemplaren als **DHCP client** (die ervoor zorgt dat je toestel automatisch een *ip-adres* kan verkrijgen – van je *router* bijvoorbeeld) en **Server** (die het delen van bestanden en printers over een netwerk mogelijk maakt). Een derde groep zit diep in het systeem genesteld en regelt de communicatie tussen Windows en allerlei toepassingen. Een van de belangrijkste vertegenwoordigers is **Remote Procedure Call (RPC)**. Groep vier levert vooral feedback over het systeem naar de gebruiker. Daartoe horen onder meer **Help en ondersteuning** (de ingebouwde helpfunctie van Windows) en **Event Log** (een systeem dat allerlei foutmeldingen en informatieve berichten van Windows en toepassingen noteert in logboeken). Een laatste reeks kunnen we onder de noemer comfortservices groeperen: services die het werken met Windows aangenamer en efficiënter kunnen maken. Typische voorbeelden zijn **Thema's** (bepalen onder meer het uitzicht van Windows) en de nieuwe **Wireless Zero Configuration-service** (laat je toe om zonder veel moeite een draadloos netwerkje op te zetten).

Manipulatie

De moraal van het verhaal? Heel wat services verrichten erg nuttig werk en vaak zijn ze

VAKTAAL | A - M | N - Z

IP-ADRES: Uniek adres bestaande uit vier getallen die door een punt gescheiden worden. Op basis van dit nummer kan een computer binnen een netwerk herkend worden.

PATCH: Betekent letterlijk 'pleister'. Stukje software dat verspreid wordt om fouten in programma's weg te werken of nieuwe functies toe te voegen.

ROUTER: Met een router worden twee netwerken met elkaar verbonden. Wordt meestal gebruikt om een lokaal netwerk (LAN) te verbinden met het internet via een breedbandaansluiting. Een router bevat een besturingssysteem om gegevens naar de juiste pc te sturen en heeft vaak ook een firewall aan boord.

Symantec AntiVirus Client	
System Event Notification	Hiermee worden systeemgebeurtenissen, zoals Windows-aanmelding, netwerk- en energiegebeurtenissen getraceerd en worden abonnees van het COM+-gebeurtenissysteem gewaarsc
System Restore-service	Hiermee worden herstelfuncties voor het apparaat uitgevoerd. Als u de service wilt stoppen, kunt u Systeemherstel uitschakelen in het tabblad Systeemherstel in Deze computer->Eigens
Task Scheduler	Hiermee kan een gebruiker geautomatiseerde taken configureren en plannen op deze computer. Als deze service wordt gestopt, kunnen deze taken niet op de geplande tijd worden uitge
TCP/IP NetBIOS Helper	Hiermee wordt ondersteuning geboden voor NetBIOS via TCP/IP (NetBT) en NetBIOS-naamomzetting inschakelen.
Telephony	Hiermee wordt ondersteuning geboden voor Telefoon-API (TAPI) voor programma's die telefoonapparaten en op IP gebaseerde spraakverbindingen bestuurd op de lokale computer en, v
Telnet	Hiermee kan een externe gebruiker zich op deze computer aanmelden en programma's uitvoeren. Deze service biedt ondersteuning voor diverse TCP/IP Telnet-clients, waaronder UNIX- .
Terminal Services	Hiermee kunnen meerdere gebruikers interactief met een bepaalde computer of het bureaublad en toepassingen van een andere computer worden verbonden. De basis voor Extern bure
Thema's	Hiermee beschikt u over een voorziening waarmee u de gebruikerservaring kunt beheren.
Uitbreidingen van het stuurprogramma vo...	Hiermee worden systeembeheergegevens doorgegeven aan en verkregen van stuurprogramma's.
Uninterruptible Power Supply	Hiermee wordt een noodvoeding (UPS) beheerd die op de computer is aangesloten
Universele Plug en Play-apparaathost	Ondersteunt hosting van universele Plug en Play-apparaten.
Verbindingsbeheer voor RAS	Hiermee kunnen netwerkverbindingen worden gemaakt.
Verwisselbare opslag	
Volume Shadow Copy	Hiermee kunnen schaduwkopieën van volumes die door back-uptoepassingen en voor andere doeleinden worden gebruikt, worden beheerd en geïmplementeerd. Als deze service wordt .
WebClient	Hiermee kunnen Windows-programma's bestanden op het Internet maken, lezen en wijzigen. Als deze service wordt gestopt, zijn deze functies niet beschikbaar. Als deze service wordt ui
Windows Audio	Hiermee worden audioapparaten voor op Windows-gebaseerde programma's beheerd. Als deze service wordt gestopt, functioneren audioapparaten en geluidseffecten niet juist. Als dez.
Windows Firewall (WF) / Internet-verbindi...	Hiermee worden services ten behoeve van netwerkadresomzetting, adressering, naamomzetting en/of preventie van onrechtmatige toegang geboden voor computers in thuis- of bedrijf.
Windows Image Acquisition (WIA)	Hiermee kunnen scanners en camera's afbeeldingen opnemen
Windows Installer	Hiermee worden toepassingen die als een Windows Installer-pakket (*.msi) worden aangeboden, toegevoegd, aangepast en verwijderd. Als deze service is uitgeschakeld, kunnen servic.
Windows Management Instrumentation	Dit is een gemeenschappelijke interface en objectmodel voor toegang tot beheergegevens over besturingssystemen, apparaten, toepassingen en services. Als deze service wordt gesto.
Windows Time	Zorgt voor de datum- en tijdsynchronisatie van alle clients en servers binnen het netwerk. Als de service is gestopt, is de datum- en tijdsynchronisatie onbeschikbaar. Als de service word.

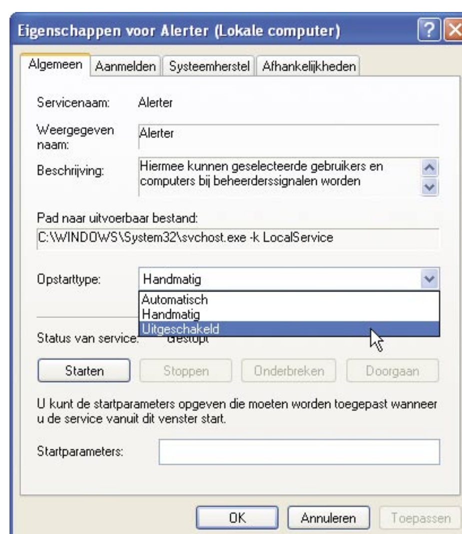
Services van allerlei pluimage...

ronduit onmisbaar! Je denkt dus best twee keer na voor je aan het sleutelen gaat. Anderzijds kunnen zulke manipulaties ook deel uitmaken van een rondje troubleshooting en zelfs van een bewuste strategie voor meer efficiëntie en veiligheid... Services snoepen namelijk ook wel wat systeembronnen af, en als je ze echt niet nodig hebt, kan je ze wellicht beter deactiveren. Maar vooral: sommige services draaien met heel wat rechten, en het zou niet de eerste keer zijn dat hackers naar veiligheidslekken speuren om die services voor eigen doeleinden te misbruiken. Zo hadden de wormen Blaster en Sasser het bijvoorbeeld op systemen gemunt met een lek in welbepaalde services, om zich op die manier te verspreiden. Services die overbodig zijn, kan je dus ook uit veiligheidsoverwegingen op non-actief zetten.

We laten je eerst zien hoe je services in het algemeen kan uitschakelen, stopzetten en opstarten, en hoe je het opstarttype wijzigt. Daarna geven we je concrete raadgevingen naar specifieke services toe.

Stop, start!

Voor onze manipulaties maken we opnieuw dankbaar gebruik van de beheermodule services.msc. Om wijzigingen in de status of het opstarttype van een service te kunnen aanbrengen, hoef je maar op zo'n service te dubbelklikken. Je belandt dan in een dialoogvenster waar standaard



Laat (voorzichtig) voelen wie de baas is!

het tabblad **Algemeen** geopend is. Stel dat je een bepaalde service tijdelijk wil activeren, dan volstaat het de knop **Starten** in te drukken. Is die uitgegrijsd, dan staat het **Opstarttype** blijkbaar ingesteld op **Uitgeschakeld**. In dat geval wijzig je het type in **Automatisch** als je die service voortaan altijd actief wil hebben, of in **Handmatig** als de activatie enkel moet gebeuren wanneer dat echt nodig is. Bevestig telkens met de knop **Toepassen**. Het wordt al iets delicater als je er aan denkt zelf een actieve service uit te schakelen. Liever dan bij **Opstarttype** meteen **Uitgeschakeld** te kiezen, roep je die service na de systeemstart via de knop **Stoppen** een halt toe. Dat doe je gedurende enkele opeenvolgende Windows-sessies. Als die ingreep na verloop van tijd geen problemen blijkt op te leveren, dan kan je het opstarttype op **Handmatig** instellen. Ga tijdens enkele sessies na of die service niet vanzelf weer actief is geworden. Is dat wel het geval, dan blijkt een ander proces die service toch nodig te hebben en schakel je die dus maar beter niet uit. Het tabblad **Afhankelijkheden** kan in dit verband al een indicatie zijn. Je leest hier namelijk niet alleen af van welke systeemonderdelen die service afhangt, maar – belangrijker nog – ook welke systeemonderdelen van die service afhankelijk zijn. Schakel je die service uit, dan liggen die afhankelijke items meteen ook op apegapen. Nemen we als voorbeeld de RPC-service: hier blijken meer dan 40 andere onderdelen zich aan vast te klampen! Experimenteer dus nooit in het wilde weg: als je een verkeerde service uitschakelt, kan dat tot grote problemen leiden! In ons kaderstukje 'Profileren' lees je trouwens hoe je met behulp van hardwareprofielen nóg veiliger aan de services kan sleutelen.

Welles, nietes

De hamvraag is natuurlijk: van welke services blijven we maar beter met onze fikken af, en welke services zijn geschikte kandidaten om met vervroegd pensioen te sturen? Geen eenvoudige vraag, want dit hangt onder meer samen met de hardware die aan je systeem hangt – heb je bijvoorbeeld geen telefoonapparaat aan je pc gekoppeld, dan kan je in principe de service **Telephony** veilig uitschakelen. Daarom hebben we in drie tabellen voorzien. In de rode tabel nemen we services op die je – vooral uit veiligheidsoverwegingen – maar beter uitschakelt. In de oranje tabel komen de twijfelaars aan bod: services die niet echt noodzakelijk zijn voor de goede werking van het systeem, en die je dus eventueel kan uitschakelen of waarvan je het type op handmatig instelt. Het is aan jou om te beslissen of je die extra functionaliteit wil missen. De groene tabel ten slotte vermeldt services die je maar beter ongemoeid laat (en dus niet uitschakelt). Hoe dan ook, schakel een service zoals hierboven beschreven best niet meteen uit, maar werk in tussenstapjes: eerst stopzetten, dan handmatig instellen en daarna pas uitschakelen.

Wil je bijkomende informatie over al deze services, dan kan je onder meer de volgende bronnen raadplegen: The Elder Geek www.theeldergeek.com/services_guide.htm, 3DSpotlight www.techspot.com/tweaks/winxp_services/print.shtml en Black Viper www.codecavalier.com/blackviper/WinXP/servicecfg.htm. Veel plezier met het sleutelwerk, maar trek wel je fluwelen handschoentjes aan! ♦

PROFILEREN

Het is perfect mogelijk de status van de services in een apart profiel onder te brengen, zodat je bij het opstarten van de pc zelf beslist met welk profiel (en dus met welke geactiveerde services) je wil opstarten. Dat is net zo veilig, aangezien je bij problemen kan heropstarten met een ander en 'braver' profiel. Daarvoor moet je dus wel eerst een zogenaamd hardwareprofiel creëren. Klik met de rechtermuisknop op **Deze computer** en kies **Eigenschappen**. Op het tabblad **Hardware** klik je vervolgens **Hardwareprofielen** aan. Druk nu op de knop **Kopiëren**, zodat je een kopie maakt van het huidige profiel (waarbij alle nodige services geactiveerd zijn). Geef die kopie een aangepaste naam en bevestig met **OK**. In dit dialoogvenster kan je meteen ook instellen hoe Windows het gewenste profiel moet kiezen bij het opstarten (bijvoorbeeld: wachten op jouw selectie). Sluit de vensters af met **OK**, en open de beheermodule voor services. Dubbelklik op elke service waarvan je de status wil aanpassen voor je tweede profiel. Op het tabblad **Aanmelden** kan je dan dit profiel selecteren en de beoogde statusknop (**Inschakelen** of **Uitschakelen**) indrukken. Bevestig opnieuw met **OK**. Bij een herstart van je pc kies je nu het gewenste profiel. Hou er wel rekening mee dat zo'n profiel voor alle gebruikersaccounts geldt. En het werken met hardwareprofielen houdt nog altijd geen vrijbrief in voor ongebreidelde experimenten! Blijf dus voorzichtig omspringen met de verschillende services.



Koppel je services aan een hardwareprofiel.

STOP!

De volgende services schakel je (onder meer uit veiligheidsoverwegingen) het best uit:

WAT IS HET?	WAT DOET HET?
ALERTER	Zorgt voor waarschuwing bij eventuele beheerdersignalen.
MESSENGER	Verstuurt berichten tussen client en server (niet te verwarren met Windows Messenger).
REMOTE REGISTRY	Maakt het mogelijk dat het register vanop een externe computer benaderd wordt.
ROUTING AND REMOTE ACCESS	Biedt routeringsdiensten aan voor LAN/WAN-omgevingen.
TELNET	Maakt het mogelijk dat een externe gebruiker zich op de pc aanmeldt en programma's uitvoert.

STOPPEN OF NIET?

De volgende services kan je eventueel aanpassen – ga na in hoeverre jij ze nodig vindt:

WAT IS HET?	WAT DOET HET?	STATUSADVIES
AUTOMATISCHE UPDATES	Maakt het mogelijk dat automatische updates gedownload en geïnstalleerd worden.	Handmatig
CLIPBOOK	Laat toe gegevens uit het plakboek te delen met externe computers.	Uitgeschakeld
DISTRIBUTED LINK TRACKING CLIENT	Onderhoudt de bestandskoppelingen.	Handmatig
DISTRIBUTED TRANSACTION COORDINATOR	Coördineert transacties die diverse bronbeheermethodes bevatten (zoals databases).	Uitgeschakeld
DNS CLIENT	Laat de computer toe zelf DNS-namen om te zetten en in een cache bij te houden.	Handmatig
IPSEC-SERVICES	Beheert het ip-beveiligingsbeleid.	Handmatig
MS SOFTWARE SHADOW COPY PROVIDER	Beheert schaduwkopieën (gekoppeld aan MS Backup-tool).	Uitgeschakeld
NET LOGON	Nodig voor authenticatie bij een domeinserver.	Uitgeschakeld
NETMEETING REMOTE DESKTOP SHARING	Hiermee kunnen externe gebruikers via NetMeeting het Windows-bureaublad benaderen.	Uitgeschakeld
PERFORMANCE LOGS AND ALERTS	Verzamelt prestatiegegevens (voor notificatie of opslag in logboeken).	Uitgeschakeld
SERVICE VOOR HET RAPPORTEREN VAN FOUTEN	Verantwoordelijk voor het venster dat een toepassings- of systeemfout rapporteert aan Microsoft.	Uitgeschakeld
SERVICES VOOR CRYPTOGRAFIE	Beheert digitale handtekeningen en certificaten.	Handmatig
SERIENUMMERSERVICE VOOR DRAAGBARE MEDIA	Geeft het serienummer van elke aangesloten draagbare mediaspeler (voor het downloaden van beveiligde inhoud).	Uitgeschakeld
SMART CARD	Beheert de toegang tot smartcards in een geschikte lezer.	Uitgeschakeld
SSDP DISCOVERY-SERVICE	Detecteert universele Plug en Play-toestellen op het eigen netwerk.	Uitgeschakeld
THEMA'S	Maakt 'thema's op het bureaublad mogelijk.	Handmatig
VOLUME SHADOW COPY	Beheert schaduwkopieën (gekoppeld aan MS Backup-tool).	Uitgeschakeld
WEBCLIENT	Laat toe dat programma's bestanden op het internet maken, lezen en wijzigen.	Handmatig
WINDOWS TIME	Zorgt voor datum- en tijdsynchronisatie binnen een netwerk.	Handmatig
WIRELESS ZERO CONFIGURATION SERVICE	Configureert de draadloze netwerkadapters automatisch.	Uitgeschakeld

DOORLATEN

De volgende services laat je best ongemoeid:

WAT IS HET?	WAT DOET HET?
(Computer Browser)	Houdt onder meer een lijst bij van computers op het netwerk.
DCOM Server Process Launcher	Zorgt ervoor dat DCOM-services kunnen draaien.
Event Log	Bewaart gebeurtenisberichten in logboeken.
Logical Disk Manager	Staat mee in voor de configuratie van vaste schijven.
Plug and Play	Laat je pc toe om wijzigingen in de hardwareconfiguratie te herkennen en zich daaraan aan te passen.
Remote Procedure Call (RPC)	Noodzakelijk voor andere RPC-services.
Windows Management Instrumentation	Geeft toegang tot beheergegevens over apparaten, services, enzovoort.
Workstation service	Zorgt voor netwerkverbindingen van clients naar servers.